电脑迷荣誉出品

黑客实战

黑客从入门到实战

黑客之门从这里开启

入侵前的踩点侦察　寻找缝隙——扫描

- 攻击Windows系统
- Web应用程序攻击
- 拒绝服务攻击
- 木马隐藏攻击
- 攻击局域网

无线网络的攻击　手机病毒攻击

后门与自身防护

齐鲁電子音像出版社

黑客实战

黑客从入门到实战

齐鲁電子音像出版社

名　　称：黑客实战——黑客从入门到实战
策　　划：彭　葵
编　　著：吴自容　王　洁　张德钢　庞　勇　张红奎　王　莉
责任编辑：于　溪
监　　制：林国刚
组版编辑：丁　洁
光盘制作：史　祺
封面设计：黄　丹

出版单位：齐鲁电子音像出版社
技术支持：（023）63658888-13101

发　　行：重庆中科普传媒发展股份有限公司发行部
电　　话：（023）63658888－13138
传　　真：（023）63659779
经　　销：各地新华书店、报刊亭
光盘生产：苏洲新海博数码科技有限公司
文本印刷：重庆现代彩色书报印务有限公司
开本规格：787×1092毫米 1/16　17.25印张 200千字

版 本 号：ISBN 978-7-900433-42-8
版　　次：2007年11月第1版
定　　价：29.80元（1CD＋手册）

版权申明

Contents 目录

第3章 攻击Windows系统

第1章 入侵前的踩点侦察

从微软不断推出新的补丁可以看出Windows系统存在漏洞，但并不是每个人都意识到自己系统存在漏洞需要打上补丁，再加上目前网络的互联互通，黑客也就由此而产生。一说起黑客，你是否觉得他们是一群行为神秘，技术高深的人？你是崇拜他们呢还是很畏惧他们？在很多人眼里，那些带着墨镜、运指如飞、坐在一台不断跳动着数据的屏幕前、一脸深沉的人就是“黑客”的标准形象。其实黑客以及黑客技术并不神秘，也并不高深。一个普通的网民在具备了一定基础知识之后，就可以成为一名黑客，甚至无需任何知识，只要学会使用一些黑客软件，就可以对网络实施攻击。

本书将向你介绍黑客常用的攻击手段和攻击方法。我们了解黑客的攻击方法，并不是用来破坏或入侵他人系统而图利，而是更懂得如何去防护自己的系统，保护自己的重要文件与数据。下面就请跟我一起进入黑客天地吧。

黑客是如何攻击目标主机的呢？当然，偶然的一次攻击可能过程就没有这么烦琐，但是如果有些机器的安全问题确实比较糟糕的话，就很有可能被黑客轻松掳为肉鸡。

黑客在攻击我们的主机时，一般会进行如下步骤：

踩点收集信息→扫描系统漏洞→攻击，这就是所谓的黑客攻击的三部曲。其中：

踩点——信息收集，是攻击之前的准备，利用ping、tracert等获取信息；

扫描——安全侦测，利用自制或专用扫描工具检测对方漏洞；

攻击——实施攻击，包括系统入侵、建立账户、获取特权、安装木马、全面攻击、留取后门等等。

下面我们将逐步进行介绍。

踩点及侦察范围概述

中国古代的大军事家孙子早在几千年前就在《孙子兵法》里指出：“知己知彼，百战不殆；不知彼而知己，一胜一负；不知彼不知己，每战必败。”对于黑客们来说，在开始攻击之前，一样需要知彼知己，他们必须摸清楚目标主机的情况，收集目标信息，针对攻击目标的特殊情况，自己需要作一些什么样的准备。就像强盗决定抢劫一家银行前，他们会事先狠下一番苦功夫收集关于这家银行的相关信息，包括武装押运车的路线和运送时间、摄像头位置和摄像范围、出纳员人数、逃跑出口甚至报警的具体位置以及其他任何有助于这次行动的信息一样，黑客在进行攻击之前也需要进行踩点，收集大量的信息，以便达到自己的攻击目的，当然由于事前做好了充分的准备工作，这种攻击才会保证自己的安全，也不会轻易被捉住。

什么是“踩点”

在入侵之前，黑客首先需要通过各种渠道摸清对方服务器的状况和当前运行的服务、系统类型等一些信息，结合使用各种工具和技巧，黑客完全可以从对某个主机从毫无所知变成知之甚详，这就是“踩点”，做到知己知彼，这样才能有清晰的思路，往往这就是决定入侵成功与否的关键所在。踩点往往是最辛苦的任务之一，但它同时也是最为重要的任务之一。

踩点进行信息收集的目的是为了进入所要攻击的目标主机。黑客通常会利用下列的公开协议或工具，收集驻留

在网络系统中的各个主机系统的相关信息。

SNMP协议 用来查阅网络系统路由器的路由表，从而了解目标主机所在网络的拓扑结构及其内部细节。

TraceRoute程序 能够用该程序获得到达目标主机所要经过的网络数和路由器数。

Whois协议 该协议的服务信息能提供所有有关的DNS域和相关的管理参数。

DNS服务器 该服务器提供了系统中可以访问的主机的IP地址表和它们所对应的主机名。

Ping实用程序 可以用来确定一个指定的主机的位置，是否开机，操作系统类型等。

如何确定大体侦察范围

当黑客决定进行攻击时，首先要解决的问题是确定踩点活动的范围。换句话说，你是打算对目标组织做全面的踩点，还是把自己的踩点活动范围控制在它的某个子公司或某个特定的地理位置？我们进行攻击的目的是什么？是以入侵系统并取得系统控制权为目的，还是窃取信息为目的，或是使目标网络或系统瘫痪为目的？目的不同，采用的攻击手段也将不同。

比如黑客在攻击ADSL用户时，就要首先确定要目标主机处于哪几个IP地址段，因为用户每次在上网时都会获得不同的IP地址，这个IP地址位于被分配的IP地址段中，整个C段IP地址的用户都是处于同一地区的。 比如想要攻击隔壁邻居的主机，则可根据自己地区的情况，适当地调节IP地址中的第二位数字，找到同一地区的上网用户IP。

未出手前先防护　代理服务器的使用

黑客在攻击过程中，为避免自己成为攻击的目标，来个“出师未捷身先死”，也为了躲避被入侵者的追查，避免自己攻击别人时被人抓到导致可能的牢狱之灾或是不必要的麻烦，一般会采取措施保护自己，掩盖自己的攻击踪迹，那么，黑客是如何掩盖自己的踪迹的呢？那就是使用代理服务器隐藏自己的IP。这样别人能看到的也就仅是代理服务器的IP地址，就无法对你实施攻击，也无法对你进行追踪了。

代理服务器的原理是在客户机和远程服务器之间架设一个“中转站”，当客户机向远程服务器提出服务要求后，代理服务器首先截取用户的请求，然后将服务请求转交远程服务器，从而实现客户机和远程服务器之间的联系。很显然，使用代理服务器后，远端服务器包括其它用户只能探测到代理服务器的IP地址而不是用户的IP地址，这就实现了隐藏用户IP地址的目的，保障了用户上网安全。

使用代理服务器的好处很多，简单概括起来主要有如下两点：

① 在上网的时候防止被入侵、攻击，因为别人看到的仅是代理服务器的网址；

② 提高网络访问的范围和速度，访问国外网站时很有用。

对于黑客来讲，使用代理服务器的最主要目的是躲避被入侵者追查，然后才是免受攻击，保证自己系统的安全性。

直接在软件中设置代理服务器

现在几乎每个跟网络有关的软件都提供“代理设置”了，只要简单设置一下就可以把真实的IP隐藏起来，取而代之的是代理IP。

目前网上的代理服务器很多，大都是免费的，只需要在Google中输入“免费代理服务器”进行搜索就可以搜索出来一大堆，图1-1所示为经常更新的免费代理服务器列表。

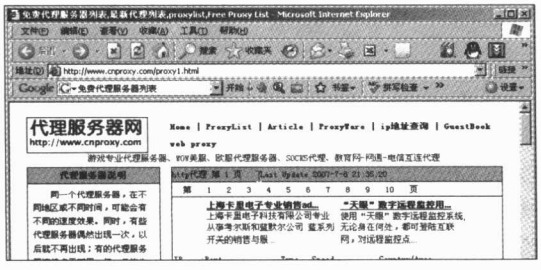

图1-1　经常更新的免费代理服务器网站

```
C:\Documents and Settings\Administrator>ping 148.240.241.67

Pinging 148.240.241.67 with 32 bytes of data:

Reply from 148.240.241.67: bytes=32 time=906ms TTL=232
Reply from 148.240.241.67: bytes=32 time=844ms TTL=232
Reply from 148.240.241.67: bytes=32 time=844ms TTL=232
Request timed out.

Ping statistics for 148.240.241.67:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 844ms, Maximum =  906ms, Average =  843ms

C:\Documents and Settings\Administrator>ping 151.8.7.15
```

图1-2　测试代理服务器速度

选择部分使用Ping命令测试一下，选择一个平均速度快一些的代理服务器，如图1-2所示。

提示

寻找免费代理服务器的方法有很多，也可以试试用ProxyHunter（代理猎手），代理服务器搜索者、QQ代理公布器XP等来搜索，它们能自动为你搜索出多个免费代理服务器，并验证各个服务器的连接速度，从而让你选择最佳途径。不过这种方法比较费时、费事，建议不到万不得已时还是不用为好。

然后再对我们最常使用的IE和QQ进行代理设置。

使用代理服务器上IE的设置方法如下：

打开IE浏览器，选择主菜单的“工具”|“Internet选项”|“连接”，然后点击下边的“局域网设置”按钮，在打开的新窗口里将“使用代理服务器”选项打上钩，然后输入代理服务器的地址和端口，如图1-3所示。

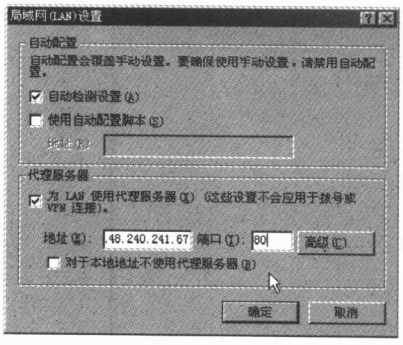

图1-3　浏览器的代理设置

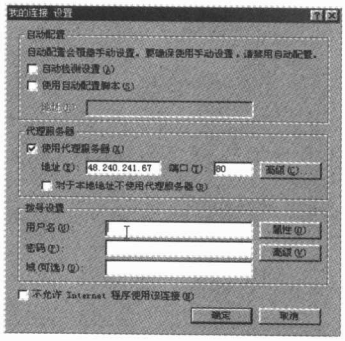

图1-4　拨号连接的代理设置

确定后关闭IE，再重启IE，就可以隐藏IP了。

如果是拨号或是ADSL拨号上网，则在“连接”选项卡中选择相应的拨号连接，再点击“设置”进行代理服务器设置，如图1-4所示。

这下黑客上聊天室或是BBS之类可以确保无忧了，因为即便有人想要查你的IP，查得结果也只是代理服务器的IP。

使用代理服务器上QQ的设置方法如下：

在QQ的系统设置中，选择“代理设置”标签项，选中“使用自定义的网络设置”项，选择“Socks5代理服务器”，输入你寻找到的免费socks5代理服务器地址，端口号一般设为1080（校验用户名和密码一般不用填），如图1-5所示。

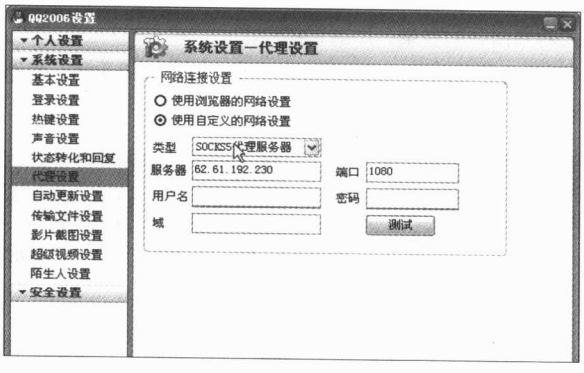

图1-5　QQ的代理设置

点击“测试”按钮，如果你填入的代理地址有效，那么会弹出“代理服务器工作正常”提示框，否则就会弹出“无法连接到代理服务器”的警告。上述步骤做完之后，最后点击“确定”完成，关闭QQ重新登录即可隐藏自己的真实IP，此后攻击者所看到的IP只是代理服务的地址。

使用代理服务器客户端软件设置

像前面介绍那样，每个程序都设置代理服务器太麻烦，要更换代理还得一个个重新设置，而且有些程序如telnet等还不方便进行代理设置。所以很多黑客会采用专门的代理服务器客户端软件来设置代理。

下面就来看看黑客如何使用代理服务器客户端软件来设置代理的。

1．利用SocksCap32

第一次启动SocksCap32时，会首先弹出“Sockscap setting”对话框，在“Socks设置”页面设置找到的代理服务器地址和端口号，并选择“Socks Version 5”协议，如图1-6所示。

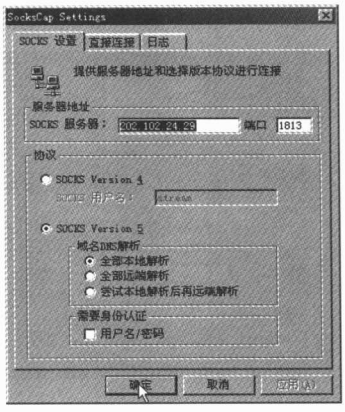

图1-6　设置代理服务器地址

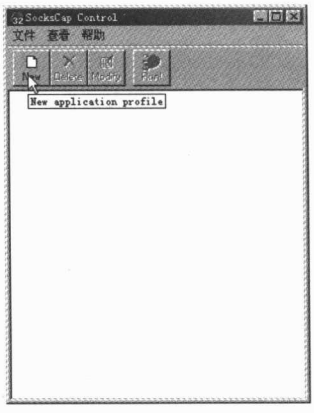

图1-7　Sockscap程序主界面

点击“确定”后进入Sockscap程序主界面，如图1-7所示。

下面我们以QQ程序为例来看看如何在SocksCap32里添加一个新程序，点击SocksCap32程序中的“文件”|“新建”命令，将弹出新建程序对话框，如图1-8所示，

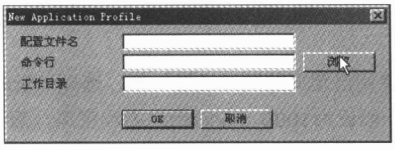

图1-8　新建程序对话框

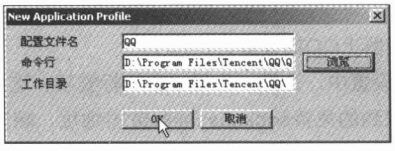

图1-9　指定QQ所在目录

点击“浏览”按钮指定QQ程序所在的目录，如图1-9所示。

最后点击“OK”按钮，QQ程序就加入到SocksCap32中了，如图1-10所示，当然最简便的方法就是将应用程序的快捷图标直接拖入主窗口。

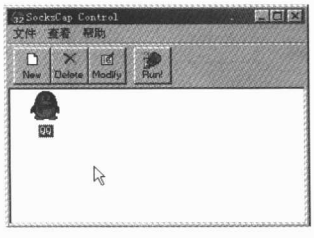

图1-10　添加进SocksCap32中的QQ程序

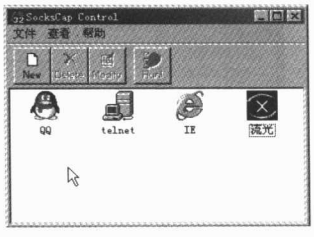

图1-11　使用代理的工具软件列表

如此类推，也可加入其它网络软件，如图1-11所示。

如果某个软件因为代理服务器设置而上不了网时，则可以选择“文件”|“设置”，在图1-6所示的对话框中重新设置一个代理服务器地址。

这样以后你上QQ时，别人利用带有查看IP补丁的QQ查看你的IP地址时，看到的也就是代理的地址，而不是你的真实IP地址了。使用流光软件进行扫描时，别人看到的也是代理服务器的地址，而不是黑客自己的真实地址了。

2.利用MultiProxy

平常收集回来的Proxy因为服务器的问题而经常更换，觉得很麻烦，所以有些黑客也使用MultiProxy软件，当一个proxy不能用的时候，它会自动转换另一个proxy，并且可以帮助检测各个proxy的速度。

下面我们就来看看MultiProxy软件具体的使用方法。

首先搜索可用的代理服务器地址。在地址栏中输入http://www.publicproxyservers.com/page1.html（这个网站的page2.html，page3.html，page4.html，page5.html都是公用代理服务器地址），虽然全是英文可能有些看不懂，不过没关系，只要将那些代理IP复制到Word中，然后再接着按下“Ctrl+Shift+F8”组合键（启用列选择模式，用于选择竖块文本），把所有代理IP以外的内容删除后，再用“替换”功能修改成形如×××.×××.×××.×××:port格式就可以了，将文件保存成TXT文件。

提示

这些代理地址大多是国外的，因为这些国外的代理针对我们上国外的网站时速度会加快，但访问国内的网站时速度可能就会减慢。如果你知道国内的代理地址，可以加入到TXT文件中的列表中，不过代理服务器的存在一般是不公开的，我们可以从聊天室或BBS站点上获得。

准备好代理服务器列表后，启动MultiProxy程序，点击主界面的“选项”按钮，如图1-12所示。

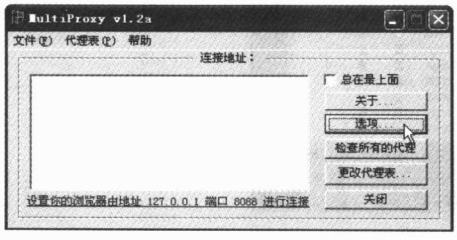

图1-12 点击主界面的“选项”按钮

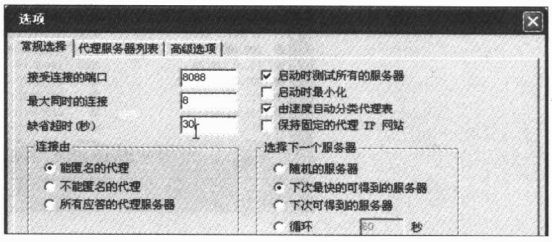

图1-13 把“缺省超时”的时间设为“30”

然后在“常规选择”页面中把“缺省超时”的时间设置长些，如设为“30”，其他设置保持不变，如图1-13所示。

再切换到“代理服务器列表”标签，选择左下角的“菜单”|“文件”|“导入代理列表”命令，如图1-14所示。

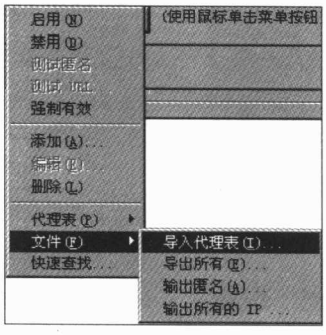

图1-14 导入代理列表

将刚才保存的代理IP文件打开，此时会弹出一个“检查代理”对话框，如图1-15所示，点按“确定”按钮，然后再按一次“确定”按钮即可返回程序主界面。

图1-15 “检查代理”对话框

提示

如果我们刚才选择的代理IP文件不能导入到列表中，可能文件中存在不符合格式的IP，将它们修改正确，保存后重新导入即可。

然后点击主界面中“检查所有的代理”按钮，验证IP是否可连接。

检验完毕后，再次单击“选项”按钮，切换到“代理服务器列表”标签，就会发现列表里有很多代理服务器，如图1-16所示。

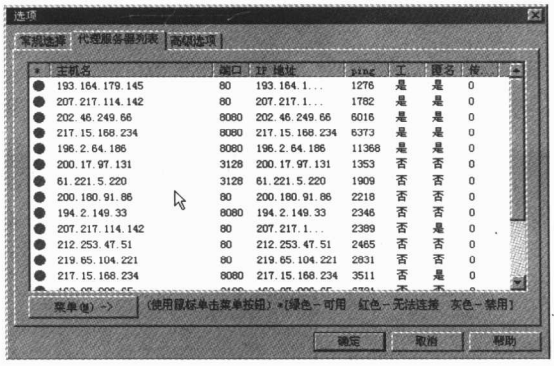

图1-16 导入的代理服务器

点击左下角的“菜单”|“代理表”|“删除没有应答的代理”命令，接着会询问“是否肯定删除所有没有应答的代理”，单击“确定”按钮，把没有应答的代理IP删除后，剩下的就是可连接的代理IP了，单击“确定”按钮返回到程序主界面。

然后启动IE浏览器（不要关闭MultiProxy）测试一下，点击“工具”|“Internet选项”命令，切换到“连接”页，这里分两种情况：

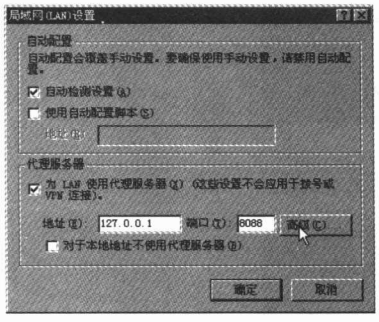

图1-17 设置代理地址

图1-18 去掉“对所有协议均使用相同的代理服务器”前的小钩